REMARKS

This communication is in response to the Office Action of July 23, 2007.

Claims 1-14 were rejected under 35 USC §103 over Tripunitara in view of Akgun.

In response to the prior art rejections Applicant has amended the claims to include a limitation for an embodiment in which the firewall is "local to a host computer station." That is, the firewall provides individual protection for a host computer station. This is supported by Figure 4, which illustrates an individual host computer station 405 includes a local firewall providing individual protection to the host computer station. As described in paragraph [0037], one benefit is that only a single computer station needs to have the firewall in order for the computer station with the firewall to be protected.

The independent claims were also amended to emphasize that the firewall issues a request for network elements having the network protocol address to reply with address resolution information in order to: "in order to check the authenticity of the unsolicited message submitting the new address resolution for the network protocol address."

New claims 15-20 were added as dependent claims reciting additional limitations on the location in which the firewall resides.

Applicant's claimed inventions permit a host computer having a local firewall to be protected from ARP spoofing attacks. As illustrated in Figure 5, when an unsolicited message is received submitting an address resolution the local address resolution cache is checked; if there is a cache hit having a different address resolution for the network protocol address, a request is made for network entities to report address resolution. The cache is updated with the submitted address resolution only if none of the reply messages include the previously cached address resolution. However, if any of the reply messages include the previously cached address resolution, the previously cached address resolution is maintained. As described in paragraph [0032] this approach acts to check the authenticity of an unsolicited new address resolution. In particular, if any other network entity reports back with the previously cached address resolution it would be an indication that the unsolicited message was likely a spoofing attack.

Applicant respectfully submits that the amended claims are patentable over the cited art. First, the Examiner on page 3 contends that the dynamic packet filter of Tripunitara corresponds to a firewall as an apparent basis for combination with Akgun. However, the dynamic packet

filter of figure 2 of Tripunitara is not in a firewall for an individual host computer station. Tripunitara teaches that Figure 2 illustrates a COIPP architecture in which a network cloud 21 is used for communication between a number of hosts 22. See e.g., column 3, lines 52-56. Tripunitara is directed to protecting an ARP cache in a gate 23 at the edge of network cloud 21. See, e.g., column 3, lines 62-66. The dynamic packet filter that the Examiner identified is illustrated as being within the network cloud 21 and is not part of the host computer 22. Moreover, Tripunitara explicitly teaches that the hosts 22 only run standard software and can't be changed, as described in column 3, lines 62-66. As Tripunitara teaches the impracticality of modifying a host to prevent ARP spoofing, one of ordinary skill in the art would not combine Tripunitara with Akgun to arrive at Applicant's claimed inventions.

Second, Tripunitara performs a completely different method of address resolution protection and therefore fails to teach many claim limitations of the pending claims. Tripunitara utilizes a modified protocol stack that resides in the network cloud at the gate to check for spoofing attacks. However, the protocol stack does not check an ARP cache. Instead, it utilizes separate queues for upward and downward flowing traffic to differentiate requests sent by a malicious host based on IP addresses. See, e.g., column 4, lines 57-60. For example column 5, lines 30-32 describes a "Requested Q in which ARP requests are remembered by recording the target IP address in the Requested Q." Tripunitara does not check an address resolution cache of the host computer and does not make additional requests for request for network entities to report address resolution for the network protocol address and then compare the replies to the submitted address resolution in order to detect spoofing.
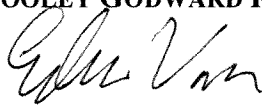
In summary, Tripunitara teaches away from a firewall local to a host computer station; Tripunitara does not check cached address resolution information of a host computer station but instead checks upward and downward queues at a gate within a network cloud; and Tripunitara does not issue requests for network elements to reply with address resolution information when it detects discrepancies with cached address resolution entries "in order to check the authenticity of the unsolicited message submitting the new address resolution for the network protocol address." Akgun is not directed to ARP spoofing attacks and thus cannot remedy the deficiencies of Tripunitara. As a result the combination of Tripunitara and Akgun fail to teach all of the limitations of Applicant's amended claims. It is therefore respectfully submitted the claims 1-20 are patentable over the combination of Tripunitara and Akgun.

It is respectfully submitted that all of the pending claims are in condition for allowance. If there are any other residual formalities that need to be resolved prior to allowing the subject application, the Examiner is requested to contact the undersigned.

The Commissioner is hereby authorized to charge any appropriate fees to Deposit Account No. 50-1283.

Respectfully submitted,
COOLEY GODWARD KRONISH LLP

Dated: _October 22, 2007_   By: _____
Edward Van Gieson
Reg. No. 44,386

COOLEY GODWARD KRONISH LLP
ATTN: Patent Group
Five Palo Alto Square
3000 El Camino Real
Palo Alto, CA 94306-2155
Tel: (650) 843-5625
Fax: (650) 857-0663

758614 v2/PA

9